forming an encrypting circuit corresponding to given encrypting specifications with at least one programmable logic device; and

reading change data for changing the encrypting specifications and automatically changing a structure of the encrypting circuit corresponding to the change data.

24. (AMENDED) A decrypting method, comprising [the steps of]:

forming [an] a decrypting circuit corresponding to given decrypting specifications with at least one programmable logic device; and

reading change data for changing the decrypting specifications and automatically changing a structure of the decrypting circuit corresponding to the change data.

~~25. (AMENDED) A signal processing method, comprising [the steps of]:~~

forming a circuit corresponding to given specifications with at least one programmable logic device; and

reading change data for changing the specifications of the circuit, the specifications representing one of encrypting specifications or decrypting specifications, and automatically changing a structure of the circuit corresponding to the change data.

REMARKS

In the March 23, 1999 Office Action, the Examiner noted that claims 1-25 were pending in the application, rejected claims 1, 5, 8, 10, 14, 17 and 19-25 under 35 U.S.C. § 102(b) and rejected claims 2-4, 6, 7, 9, 11-13, 15, 16, and 18 under 35 U.S.C. § 103(a). In rejecting the claims, U.S. Patents 4,972,478 to Dabbish; 5,703,950 to Jovanovich et al.; and 5,345,508 to Lynn et al. (References G, B and E, respectively) were cited. Claims 1-25 remain in the case. The Examiner's rejections are traversed below.

The Invention

The present invention is directed to a high-speed encrypting/decrypting apparatus. To obtain high-speed performance, a programmable logic device is used to implement the encryption/decryption specifications. When the encryption/decryption specifications change,

change data is supplied to a changing unit (represented by block 12 in Fig. 3) which causes the structure of the encryption/decryption circuit to be changed by modifying a programmable logic device therein. Several embodiments of the programmable logic device and changing unit are disclosed in the specification.

The Prior Art

U.S. Patent 4,972,478 to Dabbish

The Dabbish patent is directed to a soft logic cryptographic circuit in which an EEPROM 117 (Fig. 1) stores cipher algorithm storage instructions received from external programming equipment (EPE) 105. The EPE 105 also supplies a cipher algorithm to cryptographic cores 100, 101. As described at column 3, lines 47-61, there are no hardware or circuit changes involved, thus the title of Dabbish is accurate.

U.S. Patent 5,703,950 to Jovanovich et al.

The Jovanovich et al. patent is directed a system for controlling country specific frequency allocation within a radio frequency device. To prevent an end user from setting unapproved frequencies, each device is provided with a unique identifier and encrypted data transmitted from external sources are decrypted using this identifier.

U.S. Patent 5,345,508 to Lynn et al.

The Lynn et al. patent is directed to a system for variable-overhead cached encryption in which a temporary key is generated from an encryption/decryption key and a value to be used is changed according to the processing time and required level of security.

Rejection under 35 U.S.C. § 102(b)

In item 2 on page 2 of the Office Action, the Examiner rejected claims 1, 5, 8, 10, 14, 17 and 19-25 under 35 U.S.C. § 102(b) as anticipated by Dabbish. Reference was made to column 3, lines 44-46 as disclosing a changeable deciphering apparatus; column 1, lines 51-67 as disclosing that the changes originate from sources external to the apparatus; and part 104 as disclosing in communication circuitry which permits connection to a network. Claims 1, 10, 19, 20 and 23-25 have been amended to clarify that structural changes are made to the encrypting or decrypting circuit. Claims 21 and 22 already recited "changing

the circuit connections" (e.g., claim 22, lines 6-7). As discussed above, no suggestion of making structural changes have been found in Dabbish. Therefore, it is submitted that claims 1, 10, 19, 20-25 and claims 5, 8, 14 and 17 which depend therefrom patentably distinguish over Dabbish.

Rejections under 35 U.S.C. § 103(a)

In item 4 on pages 3-4 of the Office Action, claims 2-4, 6, 11-13 and 15 were rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish in view of Jovanovich et al. None of the features described in item 4 as being taught by Dabbish and Jovanovich et al., or sufficiently well-known to take Official Notice, include structural changes to a circuit as now recited in claims 1 and 10. Since claim 2-4 and 6 depend from claim 1 and 11-13 and 15 depend from claim 10, it is submitted that claims 2-4, 6, 11-13 and 15 patentably distinguish over Dabbish in view of Jovanovich et al. for the reasons discussed above with respect to claims 1 and 10.

In item 5 on page 4 of the Office Action, claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish. Since claims 7 and 16 depend from claims 1 and 10, respectively, it is submitted that claims 7 and 16 patentably distinguish over Dabbish for the reasons set forth above with respect to claims 1 and 10.

In item 6 on pages 4-5 of the Office Action, claims 9 and 18 were rejected under 35 U.S.C. § 103(a) as unpatentable over Dabbish in view of Lynn et al. Nothing in the cited portions of Lynn et al. teach or suggest modifications of a circuit, so that high-speed encryption and decryption can be performed for different encryption and decryption specifications. Since claims 9 and 18 depend from claims 1 and 10, respectively, it is submitted that claims 9 and 18 patentably distinguish over the combination of Dabbish in view of Lynn et al. for the reasons set forth above with respect to claims 1 and 10.

Other Cited Art

Five U.S. patents were cited but not used to reject the claims. As recognized by the Examiner, these references do not teach or suggest the features of the present claimed invention. U.S. Patent 5,768,372 to Sung et al. (Reference A) discloses an apparatus for

securing programming data of a programmable logic device using decompression and decryption circuits, but not modifying encryption and decryption circuits by changing the programming of a programmable logic device. U.S. Patent 5,623,637 to Jones et al. (Reference C) is directed to a smart card with an access password and encryption keys. U.S. Patent 5,388,157 to Austin (Reference D) is directed to providing security of data in an EEPROM device. U.S. Patent 4,386,234 to Ehrsam et al. (Reference H) is directed to terminals that perform cryptographic communication and provide for file security.

Summary

It is submitted that the references cited by the Examiner, taken individually or in combination, do not teach or suggest the features of the present claimed invention. Thus, it is submitted that claims 1-25 are in a condition suitable for allowance. Reconsideration of the claims and an early Notice of Allowance are earnestly solicited.

If any further fees are required in connection with the filing of this Amendment, please charge same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 31,106

Suite 500
700 Eleventh St., N.W.
Washington, D.C. 20001
(202) 434-1500

Date: 6/23/99